



Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 12 December 2003

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The Securities Investor Protection Corporation reports investors and brokers need to be on their guard against a new fraud scheme in which con artists are falsely posing on the Web as authentic brokerage firms that are members of the SIPC. (See item [6](#))
- The Associated Press reports the Trust for America's Health has published a report that says states are only moderately prepared to handle bioterror, and thirty-two states have even cut their spending on public health. (See item [17](#))
- eWEEK reports that a new vulnerability in Internet Explorer could allow for the spoofing of URLs in the Web browsing, potentially putting users' sensitive information at risk. (See item [22](#))

DHS/IAIP Update *Fast Jump*

Production Industries: [Energy](#); [Chemical](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [General](#); [DHS/IAIP Web Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *December 11, Indianapolis Star (IN)* — **Midwest ISO is improving training and alerts.** A Carmel, IN-based electrical grid monitor heavily criticized in last summer's massive blackout is increasing training and monitoring in an effort to prevent a recurrence, the company's leader said Wednesday, December 11. **James Torgerson, president and chief executive officer of the Midwest Independent System Operator (ISO), said the company has improved alarms**

and other systems so it can respond to problems more quickly. In addition, the 2-year-old not-for-profit company has nearly finished negotiating an agreement to communicate better and work more closely with a neighboring grid monitor in the Northeast, PJM Interconnection. The U.S.-Canadian task force's report last month on the blackout said it could have been contained with better monitoring by Midwest ISO and better communication. The company will take another step Jan. 1 when it begins using a computer system that monitors its coverage area every five to 10 minutes, providing more up-to-the-minute information. It will keep track of energy load and reliability at 35,000 points in the parts of 15 states that Midwest ISO monitors. The computer, called a State Estimator, also will try to anticipate problems by testing more than 5,000 possible changes in the system and what might result from them.

Source: <http://www.indystar.com/articles/4/101170-5964-009.html>

[\[Return to top\]](#)

Chemical Sector

Nothing to report.

[\[Return to top\]](#)

Defense Industrial Base Sector

2. *December 11, Aerospace Daily* — Rumsfeld says more work needed on cruise missile defense. Department of Defense (DoD) Secretary Donald Rumsfeld said Wednesday, December 10, that the United States needs to do more to defend the homeland and deploy troops against cruise missiles. While most of DoD's missile defense programs are focused on defeating ballistic missiles, cruise missiles are increasingly attractive to U.S. enemies because they are widely available, "not terribly expensive," and can be launched from ships, said Rumsfeld. Although Rumsfeld proposed no new initiatives, he expressed confidence that such programs as the Medium Extended Air Defense System (MEADS), which is being developed to protect troops against cruise and ballistic missiles, will be robustly funded in the future. Kenneth Knight, chief of the Defense Intelligence Agency's Defense Warning Office, said that anti-ship cruise missiles remain a "very significant challenge" but that foreign countries are shifting their emphasis to land-attack cruise missiles (LACMs). Nearly 70 percent of current cruise missiles are anti-ship, but almost half of cruise missiles under development are land-attack. Knight said nine countries now are producing LACMs or key components.

Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/rum12113.xml

3. *December 11, Reuters* — U.S. reports successful sea-based missile shield test. A missile from a U.S. Navy Aegis cruiser knocked out a dummy warhead over the Pacific Thursday, December 11, the fourth intercept in five such tests of a sea-based anti-missile shield, the Pentagon said. The Standard 3 missile fired from the Lake Erie off Kauai in the Hawaiian islands "successfully engaged the target with hit-to-kill technology" about four minutes after the target was launched, said Chris Taylor, a spokesperson for the Pentagon's Missile Defense Agency. The test was designed to evaluate selected long-range surveillance and track

functions of the Aegis system, the Missile Defense Agency said. The last test, on June 18, failed. The sea-based defense is to be integrated into a multilayered missile shield.

Source: http://biz.yahoo.com/rc/031211/arms_missile_test_1.html

[[Return to top](#)]

Banking and Finance Sector

4. *December 11, South African Press Association* — **UK bank fined for money laundering.** Abbey National, Britain's second-biggest mortgage lender and the country's sixth-biggest bank, was fined a record \$3,543,648.79 USD by the Financial Services Authority on Wednesday, December 10, for serious compliance failures, including breaches of money laundering rules. The authority imposed a \$3,487,731.69 USD penalty on Abbey National for failing to maintain effective anti-money laundering procedures and imposed a \$558,013.65 USD penalty on the group's asset managing business for separate systems and control breaches. **An investigation by the authority found that Abbey National failed to ensure that suspicious activity reports in its retail banking division during December 2001 and April 2002 were promptly considered and reported to the National Criminal Intelligence Service.** The authority introduced strict money laundering rules in December 2001 as part of the global crackdown on the funding of terrorist activities. "The failure by Abbey National to monitor compliance with the authority's money laundering rules demonstrated a marked lack of regard for its regulatory obligations," said Andrew Procter, the director of enforcement at the authority. Abbey National said it would not appeal, and had already taken action to address the issues identified.

Source: <http://www.busrep.co.za/index.php?fSectionId=565&fArticleId=305992>

5. *December 11, PC Pro* — **E-mail banking scam moves on to Lloyds TSB.** The e-mail scam that spoofed a security announcement from UK bank Natwest on Monday, December 8, has now moved on to Lloyds TSB. The e-mail, which has been sent to both customers and non-customers of the bank, reads, "Our new security system will help you to avoid frequently fraud transactions and to keep your investments in safety...Due to technical update we recommend you to reactivate your account." The poor use of language is an indication of a scam e-mail, however the associated graphics give the e-mail a professional appearance. If a recipient of the e-mail clicks the link as requested, they are taken to a page that requests personal information. **A spokesperson for the bank said that a new element to the scam is the request for "memorable information." This is a nine digit numerical sequence that Lloyds TSB requests customers to enter in random positions in the sequence to authenticate themselves.** However the scam asks for all nine digits. The spokesperson said Lloyds TSB would not ask for that information in full.

Source: http://www.pcpro.co.uk/?http://www.pcpro.co.uk/news/news_story.php?id=51291

6. *December 11, Securities Investor Protection Corporation* — **SIPC issues warning about Web-based 'brokerage identity theft' targeting investors.** Investors and brokers need to be on their guard against a new fraud scheme in which con artists are falsely posing on the Web as authentic brokerage firms that are members of the Securities Investor Protection Corporation (SIPC), which maintains a special reserve fund to protect the customers of insolvent brokerage firms. The SIPC issued a public warning on Thursday,

December 11, about brokerage identity theft. **The scheme usually works by con artists setting up a Website that uses the name of an actual SIPC member brokerage firm, but with a different address. In other cases, the party committing the fraud uses the name of an actual registered broker, and then sets up a bogus entity using that person's name and address.** The fictional internet entity claims to be a respected brokerage firm, and a member of SIPC. The victim is often told to check the membership database on SIPC's Website, in order to "prove" that the firm is a SIPC member, when in fact the fictional firm has simply stolen the identity of a real SIPC member. SIPC President Stephen Harbeck said, "SIPC has recently received information from more than a dozen U.S. and non-U.S. victims of this type of fraud."

Source: http://biz.yahoo.com/prnews/031211/dcth019_1.html

[\[Return to top\]](#)

Transportation Sector

7. *December 11, Associated Press* — **South Carolina receives \$9 million to bolster port security.** "Port security is one of our top concerns in South Carolina," said U.S. Sen. Lindsey Graham, R-SC. He added that the state's ports play an important role in the economy. The money awarded this week includes \$5.2 million from the U.S. Department of Homeland Security. That money will go to the South Carolina State Ports Authority and other terminal operators to improve security. **Another \$3.8 million grant from the Office of Domestic Preparedness will go to the Charleston County Sheriff's Office to buy equipment to further improve security around the Port of Charleston. Some of that money will be used to purchase a robot and a containment vessel which can transport biological and chemical weapons.** "The Port of Charleston is a critical national asset, and protecting that asset is both a national and a local responsibility," said Charleston County Sheriff Al Cannon. "This puts us in a better position, from an equipment perspective, to do the kind of things we have to do to assure the safety of the port and the community that surrounds it."

Source: <http://www.thestate.com/mld/thestate/news/local/7468224.htm>

8. *December 11, Associated Press* — **Long Beach-LA ports awarded \$17 million for security. The Department of Homeland Security funds will be used for perimeter barriers, surveillance, cargo inspection and detection systems, port officials and lawmakers said.** Since the 2001 terrorist attacks, port officials and federal lawmakers have pressed for additional security funding for the ports, which combined handle more than a third of the nation's international container shipping. **Homeland Security Secretary Tom Ridge on Wednesday announced that a total of \$33.7 million was awarded in port security grants statewide and \$179 million nationwide.**

Source: <http://www.nbc4.tv/news/2698638/detail.html>

9. *December 11, Associated Press* — **Bridgeport, CN, receives money for harbor security.** The Department of Homeland Security is awarding more than \$3 million in grants to bolster anti-terrorist measures at Bridgeport Harbor. **Most of the money has been awarded to the Bridgeport Port Authority, which plans to spend it on video surveillance equipment, fencing and lighting for its facilities.** "Basically, we are going to increase security measures in Bridgeport Harbor at the ferry terminal and the Bridgeport regional maritime complex, which is home to Derecktor Shipyards," said Joseph A. Riccio Jr., executive director of the port

authority. Hundreds of thousands of dollars are being sent to New Haven for port security there.

Source: <http://www.nbc30.com/politics/2698956/detail.html>

10. *December 11, Associated Press* — **Amtrak request to block walkout rejected.** A federal judge rejected Amtrak's request to block a threatened one-day walkout by railroad unions to protest what they say is chronic underfunding of passenger rail. **Unions representing 8,000 of Amtrak's 21,000 employees had planned the work stoppage for October 3, but agreed to postpone any action until the court ruled.** Though the unions can proceed, they have not said whether or when they will do so. The stalemate over federal funding they hoped to address with their one-day protest has been broken, at least for this year. The Transportation Communications Union, which represents about half of Amtrak's unionized employees, has previously said it wouldn't participate in a stoppage. U.S. District Judge James Robertson, in his ruling issued Wednesday and posted Thursday, denied Amtrak's request for an injunction. The passenger railroad failed to prove that the union was planning an "unlawful act," the judge wrote. Amtrak already has appealed to the U.S. Court of Appeals, railway spokesman Cliff Black said. **Amtrak claims the railroad has a legal and public service obligation to provide intercity passenger rail service every day. Black said a one-day walkout would likely shut down Amtrak's nationwide system and undermine the railroad's support in Congress.**

Source: <http://www.cnn.com/2003/TRAVEL/12/11/bi.amtrak.walkout.ap/>

11. *December 11, Associated Press* — **Amtrak strike would affect VRE, MARC. If Amtrak workers go ahead and strike, commuters on Virginia Railway Express (VRE) and MARC trains will also be disrupted. Amtrak runs both VRE lines and the MARC Penn Line.** MARC spokesman Richard Scher tells The Associated Press the impact would depend on which unions walk out. The Penn Line is MARC's most traveled — averaging about 16,000 trips a day. But since Amtrak owns Union Station, in Washington, DC, that could also hit the Brunswick and Camden Lines. Scher says they'd try to run those trains at least as far as a Metro station. At VRE, spokesman Mark Roeber says an Amtrak strike would likely shut them down, since Amtrak provides both crews and maintenance. More than 15,000 riders use the Manassas and Fredericksburg lines. Roeber says a strike in January would be worse than in December, when the holidays keep ridership lighter than normal. A federal judge today cleared the way for Amtrak workers to hold a one-day strike to protest what they say is a lack of support from the White House and Congress.

Source: <http://www.wjla.com/news/stories/1203/113596.html>

[\[Return to top\]](#)

Postal and Shipping Sector

Nothing to report.

[\[Return to top\]](#)

Agriculture Sector

12. *December 11, Independent Record (Montana)* — **No trace of CWD found in deer, elk samples.** None of the more than 1,000 samples of deer and elk tissue so far tested, in Montana,

this fall for the deadly chronic wasting disease (CWD) came back positive, wildlife officials say. **Hunters submitted some 1,600 samples of deer and elk tissue this past hunting season, said Ron Aasheim of the Montana Fish, Wildlife and Parks Department. So far, 1,030 have been processed, and all have come back negative.** The rest are still being processed. "It's certainly good news," he said. "But as we've said in the past, we certainly expect that at some point, we're going to find CWD in Montana. It surrounds us on three sides." Once confined to pockets of Wyoming, Colorado and Nebraska, the CWD is now widespread across much of the West and Midwest. This year, samples came from all parts of the state, but officials tried to get more samples in the areas where the disease is most likely to show up: along borders with states or provinces known to have the disease and around Philipsburg, where the disease was found before.

Source: http://www.helenair.com/articles/2003/12/11/montana/a07121103_01.txt

13. *December 11, Food Production Daily* — **Classical swine fever test.** The European Commission Wednesday approved a new test to be used after vaccination against classical swine fever (CSF). **This scientific breakthrough will make it possible, in case of emergency vaccination with a marker vaccine, to distinguish vaccinated pigs from pigs naturally infected with CSF.** This distinction is not possible when using conventional vaccination. This new development could have enormous benefits for meat processors. Classical swine fever is a viral infection of domestic and feral pigs that causes a serious disease with very high mortality. EU measures for the control of CSF include the possibility to make use of vaccines in case of an emergency. However, their use is seriously hampered by the possibility that, in case of CSF infection, vaccinated pigs may then further spread the disease, but cannot be distinguished from those that are vaccinated but not infected. Therefore, certain prevention measures are necessary to avoid the further spread of disease from the areas where vaccine is used. These measures include restrictions on the trade in vaccinated pigs and their products which reduces the viability of vaccination for disease control.

Source: <http://www.foodproductiondaily.com/news/news-NG.asp?id=48386>

[\[Return to top\]](#)

Food Sector

14. *December 11, Food and drug Administration* — **FDA and CBP announce transitional compliance policy on food imports.** The Food and Drug Administration (FDA) and the Bureau of Customs and Border Protection (CBP) Tuesday issued a compliance policy guide that describes their strategy for maintaining an uninterrupted flow of food imports while improving their safety in accordance with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002. The policy guide deals with the enforcement of the Bioterrorism Act's requirement, which becomes effective on December 12, 2003, that FDA receive a prior notification of all human and animal food, drinks and dietary supplements imported or offered for import to the U.S. As the rule becomes effective, FDA and CBP expect a "good faith" effort at compliance. **The policy guide issued today makes clear that during the next 8 months, the two agencies will primarily rely on educating the affected firms and individuals. During this period, the agencies will utilize communication and education initiatives, escalating imposition of civil monetary penalties, and ultimately refusal of shipments. This phase-in period will end on August 12, 2004.** The compliance guide is

available at: <http://www.cfsan.fda.gov/~pn/cpgpn.html>.

Source: <http://www.fda.gov/bbs/topics/NEWS/2003/NEW00995.html>

15. *December 11, Associated Press* — **Law to protect food supply takes effect. Food exported to the U.S. will be more closely examined as of Friday under new rules to thwart bioterrorists.** Under the Bioterrorism Act, the U.S. government requires 400,000 food handling companies to register all products with the Food and Drug Administration (FDA). **The FDA said that as of Wednesday, two days before the new regulations take effect, 131,000 food handling companies had registered, about 68,000 of which were outside of the United States.** Mexican customs broker Janet Martinez said many of her clients are not even aware of the new law. She doubts they will meet the new requirements. "In Mexico, there are places where there isn't even a phone," Martinez said. "A lot of our clients are small producers and they are not at the level to comply with what the FDA is asking." In India, exporters say the new rules could result in product losses. Subodh Shah, deputy manager of international marketing for a company that exports frozen foods to the U.S., said his products must be kept at near freezing temperatures. Delays at ports of entry could cost him entire shipments. Kazim Gurel, deputy chairman of the board of a Turkish company which exports spices to the U.S., said the biggest headache for him will be additional paperwork. "At the end of the day, there will be added documentation," he said. "But I wouldn't say it's a barrier to trade."

Source: <http://famulus.msnbc.com/FamulusIntl/ap12-11-105451.asp?reg=AMERICAS>

[[Return to top](#)]

Water Sector

16. *December 11, South Florida Sun-Sentinel* — **Florida farmers offer land for water storage.** Florida farmers are offering to use their ponds and empty fields to store storm water to help avert ecological damage to the overfilled Lake Okeechobee and coastal estuaries. **In an unprecedented plan, billions of gallons of water from Lake Tohopekaliga and Lake Okeechobee would be diverted to private farm land.** Some water already has been moved to the Seminole Indian reservation and into remote wetlands in southwestern Palm Beach County. The water transfers should offset discharges that began November 10 from a 30-square-mile lake nicknamed Toho near Kissimmee. The Florida Fish and Wildlife Conservation Commission touted the releases as a vital step for its \$8 million restoration of Lake Toho. The water would provide an agricultural benefit by seeping into the ground to raise water tables that nourish crops, district officials said. The water district calculates the Toho discharges could lift brimming Lake Okeechobee about 1.2 inches after flowing down the Kissimmee River. Some of the private land lined up is positioned to intercept some Toho water while other properties would absorb water from 730-square-mile Lake Okeechobee so it would not rise and spill into the St. Lucie River estuary.

Source: http://www.sun-sentinel.com/news/local/palmbeach/sfl-pfarmer_s11dec11_0.3625536.story?coll=sfla-news-palm

[[Return to top](#)]

Public Health Sector

17. *December 11, Associated Press* — **Report: States only moderately prepared to handle bioterror. Thirty-two states have cut their own spending on public health even as Congress sent massive federal aid to shore up state systems, the report found.** The U.S. Centers for Disease Control and Prevention (CDC) does no tracking to ensure that states are using the federal money to supplement, not supplant, their own public health spending, said the nonprofit Trust for America's Health, which released the report Thursday. In many states, the federal grants themselves have been caught up in red tape that limits how much has reached local authorities, the report said. **One result: By the government's own measure, only Florida and Illinois are fully prepared to distribute and administer vaccinations and antidotes shipped from the nation's emergency stockpile in the event of a bioterrorist attack.** The overall money crisis has even greater implications, because the same basic systems crucial to battling bioterrorism are needed for today's health emergencies. Yet only 13 states have plans for how to handle a flu pandemic. **Next year, the CDC will begin the first comprehensive assessment of how well every state is prepared for bioterrorism and other health emergencies.**

Source: http://www.usatoday.com/news/nation/2003-12-11-states-bioterror_x.htm

18. *December 11, BBC News* — **Epidemic threat of minor bugs. Experts have calculated that some bugs are gaining enough of a foothold in humans to pose a significant threat. They predict epidemics are "waiting to happen."** There are many pathogens which cause only a handful of cases within outbreaks. The researchers in this study, from Emory University, the University of Washington, and Universite Pierre and Marie Curie in Paris, have worked out a way of calculating the risk from each pathogen. **They can calculate an "emergence" factor by observing when a case of the illness in humans happens, and counting how many other people catch the infection as a result of just a single case. The higher the number, the more likely it is that the pathogen could be dangerous on a global scale. This is because, the more people who carry the pathogen, the more opportunities it has to undergo a genetic mutation into an organism better suited to preying on humans.** Changes in this factor could also happen because of increases in population density or living conditions which may lead to greater transmission. They say that eradicated diseases, such as smallpox, could return in other forms as immunity in the world population begins to dwindle.

Source: <http://news.bbc.co.uk/1/hi/health/3307847.stm>

19. *December 11, Agence France Presse* — **Drug-resistant bacteria spread in France. A highly resistant bacteria which has spread through several hospitals in northern France has killed 18 people since July,** according to a statement from the health ministry Wednesday. **More than 20 hospitals have reported the presence of the super-bug, Acinetobacter Baumannii, which causes breathing problems in patients already weakened by other illnesses and is unaffected by most antibiotics,** the ministry said. A total of 112 cases have been detected, but the number is falling off as a result of a strict hygiene regime, the ministry said. The French health system is under growing scrutiny after it failed to prevent more than 15,000 deaths in last summer's heatwave. It is suffering a severe manpower shortage as a result of the reduced 35-hour working week introduced by the last Socialist government.

Source: http://www.expatica.com/source/site_article.asp?subchannel_id=58&story_id=3073

[[Return to top](#)]

Government Sector

Nothing to report.

[\[Return to top\]](#)

Emergency Services Sector

20. *December 11, Argus Online* — **Twenty-second quake warning best science can offer before a major earthquake strikes.** But it is enough, scientists and emergency responders said to save lives, direct the initial response and avert some of the chaos when the Earth next shakes. **The warning, scientists say, is possible only because they can now work faster than an earthquake's shockwaves roll through the ground. Remote sensors pick up the first signs of a temblor and computers pinpoint location and magnitude.** "Every second counts," said Ta-liang Teng, a University of Southern California professor and seismologist with the Southern California Earthquake Center. Speaking at the fall meeting of the American Geophysical Union, an annual gathering of nearly 10,000 scientists from around the world, Teng and other scientists said **even the most advanced early warning system affords time enough to trigger only automated responses — stopping trains, for instance, or shutting a refinery.** "It's questionable whether a nuclear power facility could power down, even with the longest of warning periods." And places such as the Los Angeles basin or the East Bay would be out of luck — scientists need about 45 miles separating the epicenter from a major metropolitan area.

Source: <http://www.theargusonline.com/Stories/0,1413,83~1971~1823434,00.html>

21. *December 11, Gulf News (Dubai)* — **Thousands flee Iran city after gas leak.** Sixty per cent of residents in the southern city of Masjed Soleiman have been either evacuated or forced to leave following reports of a poisonous gas leak from a rusty, non-standard pipeline. **There are 150,000 people living in Masjed Soleiman, which is dotted with several oil wells, most of them no longer operational and giving off poisonous gases. The dangerous fumes have created problems for the residents, particularly children.** "The leakage of poisonous gases has been a problem for the residents for a long time. Non-operational wells and the rusty oil pipelines are the root cause of the problem," Satar Akbar Zadeh, Governor of Masjed Soleiman, told Gulf News. People are fleeing the city to the suburbs or nearby cities and seeking shelter in the homes of relatives or friends. "A team of three physicians and two chemical experts have come to the city from Shiraz to investigate the case," said Akbarzadeh, stressing there is no danger of an explosion. **Seyed Abdullah Mousavi, Managing Director of the Oil and Gas Company of Masjed Soleiman, told Gulf News that negligence in the process of burning liquid gases was the main cause of the leakage.** The gas accumulated in a gas well outside Masjed Soleiman leaked while it was being transferred to the "burning cavity" at the centre of town to be burnt.

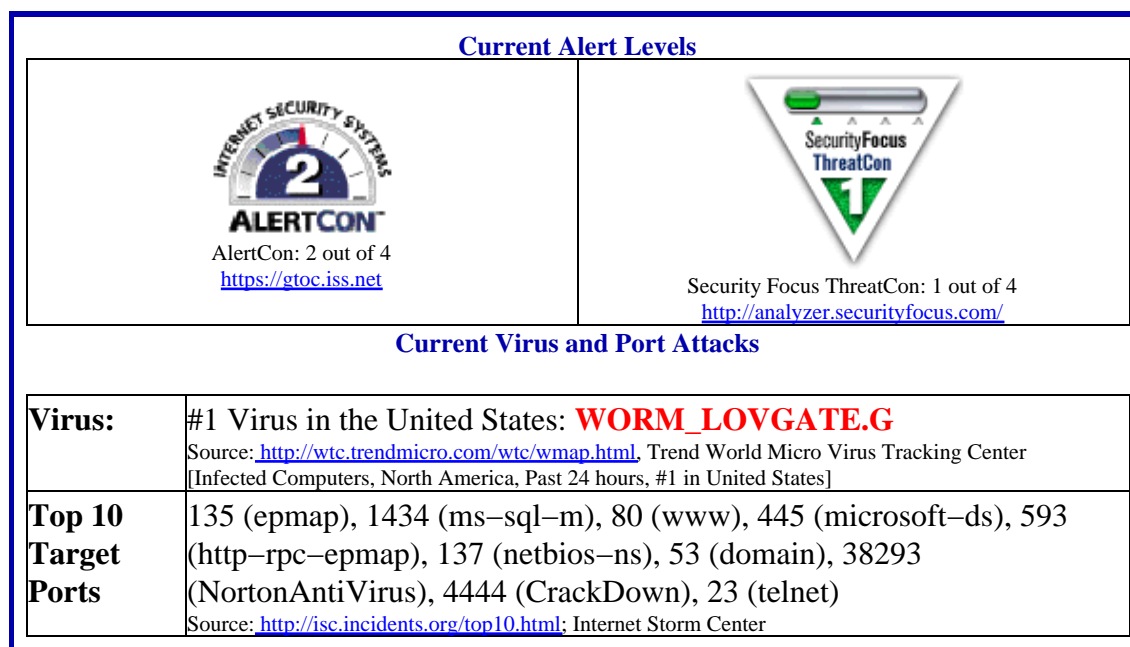
Source: <http://www.gulf-news.com/Articles/news.asp?ArticleID=105192>

[\[Return to top\]](#)

Information and Telecommunications Sector

22. *December 12, eWEEK* — Internet Explorer spoofing vulnerability found. Security researchers confirmed a vulnerability in Internet Explorer 6 Tuesday, December 9, that could let an attacker display a fake URL in the browser's address bar in an attempt to disguise the real domain, an advisory from security company Secunia Ltd said. Using the security hole, an attacker could trick users into providing sensitive information or download malicious software by leading them to think that they are visiting a trusted site, the advisory said. A Microsoft spokesperson on Wednesday said that the company knows of no exploits of the reported hole or of any users being affected but said in a statement that it is "aggressively investigating the public reports." Microsoft may provide a fix through its monthly patch release cycle or a separate patch, depending on the outcome of the investigation, the spokesperson said. The Secunia advisory is available here: <http://www.secunia.com/advisories/10395>
Source: <http://www.eweek.com/article2/0.4149.1409620.00.asp>

Internet Alert Dashboard



[\[Return to top\]](#)

General Sector

23. *December 11, Reuters* — German anti-militant raid. Over 5,500 German police took part in a raid against militant Islamists in a nationwide crackdown on alleged members of a banned extremist organization. The swoop Thursday, in 13 of Germany's 16 states, centered on over a thousand suspected members of the group known as the Kalifatstaat, which the government outlawed in 2001 as unconstitutional and a threat to democracy. The Federal Crime Agency (BKA) said the suspects targeted were subscribers to the group's newspaper, "Beklenen Asr-I Saadet," and that an unspecified number of arrests had been made. "Weapons, propaganda material, computers, and mobile phones have been confiscated," a BKA spokesman said. "There have also been a number of arrests." The swoop focused on the states

of North Rhine–Westphalia and Baden–Wuerttemberg, where some 660 premises were raided. **Federal prosecutor Kay Nehm also said he was investigating four members of the Kalifatstaat on suspicion of planning attacks and creating a terrorist organization.** Nehm also ordered a search of the premises of the group's leader, Metin Kaplan, known as the "Caliph of Cologne," on the grounds he was continuing to direct the Kalifatstaat.

Source: <http://edition.cnn.com/2003/WORLD/europe/12/11/germany.islam.ic.reut/>

[[Return to top](#)]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web-site (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings – DHS/IAIP Assessments, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications – DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive – Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions: nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703–883–6631

Subscription and Distribution Information: Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703–883–6631 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202–323–3204.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open–source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.